




DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	POLICY NO. 500.21	EFFECTIVE DATE 2/15/2013	PAGE 1 of 7
APPROVED BY:  Director	SUPERSEDES 500.21	ORIGINAL ISSUE DATE 4/14/2003	DISTRIBUTION LEVEL(S) 1

PURPOSE

- 1.1 To establish safeguards that must be implemented by the Los Angeles County-Department of Mental Health (LAC-DMH or Department) in order to protect the confidentiality of Protected Health Information (PHI).

DEFINITIONS

- 2.1 **Protected Health Information (PHI):** Is information that is (i) created or received by a health care provider, health plan, employer or health care clearinghouse; (ii) relates to the past, present or future physical or mental health condition of an individual, the provision of health care to an individual, or the past, present or future payment or the provision of payment of individual; and (iii) identifies the individual for which there is a reasonable basis for believing that the information can be used to identify the individual.
- 2.2 **Particularly Sensitive Health Information:** PHI that is generally considered highly confidential including, but not limited to, mental health, substance abuse, genetics, and sexually transmitted disease information, including HIV/AIDS.
- 2.3 **Workforce:** Employees, volunteers, trainees and other persons whose conduct in their work is under the direct control of LAC-DMH, whether or not they are paid by the County.
- 2.4 **Landline Telephone:** Refers to a telephone which uses a solid telephone line such as metal wire or fiber optic cable for transmission.

POLICY

- 3.1 Set forth below are policies establishing minimum administrative and physical standards regarding the safeguarding of PHI that will be enforced by LAC-DMH. The Department may develop additional policies and procedures that are stricter than the parameters set forth below in order to maximize the safeguarding of PHI in support of their specific circumstances and requirements. The development and implementation of policies and procedures in addition to those stated herein must be approved by the Los Angeles County Chief HIPAA Privacy Officer.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	POLICY NO. 500.21	EFFECTIVE DATE 2/15/2013	PAGE 2 of 7
--	---------------------------------	---	---------------------------

- 3.2 LAC-DMH will implement appropriate administrative, technical and physical safeguards which will protect PHI from any intentional, unintentional or incidental use or disclosure that is in violation of the Department's Privacy Policies or the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. This requirement applies to all types of PHI in any form, i.e., oral, paper or electronic.
- 3.3 The Department workforce must reasonably safeguard PHI to limit incidental use or disclosure made pursuant to an otherwise permitted or required use or disclosure.

PROCEDURES

4.1 Administrative Safeguards

- 4.1.1 Incidental/Oral Communications: The Department's workforce must exercise due care to avoid unnecessary disclosure of PHI through oral communications. Conversations in public areas should be avoided unless necessary to further client care, research, or teaching purposes. Voices should be modulated and attention paid to unauthorized listeners in order to avoid unnecessary disclosure of PHI. Client identifying information should be disclosed during oral conversation only when necessary to further treatment, payment, teaching, research, or operational purposes. Dictation and telephone conversations should be conducted away from public areas if possible. Speakerphones should be used only in private areas. Computer monitors, printers, fax machines, whiteboards and any other equipment that displays PHI should be placed where passers-by cannot see them. The type of PHI found on a sign-in sheet or included when paging a client should be limited to the least amount of information necessary to accomplish the purpose.
- 4.1.2 Cellular Telephones: The use of cellular telephones is not prohibited as a means of using or disclosing PHI. However, their use poses a higher risk of interception as compared to landline telephones. Landline telephones should be used if the conversation will involve the disclosure of PHI. Use of cellular devices must comply with DMH Policy No. 307.02, Assignment, Use, and Management of Cellular Devices. (See Reference 1)



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	POLICY NO. 500.21	EFFECTIVE DATE 2/15/2013	PAGE 3 of 7
--	---------------------------------	---	---------------------------

4.1.3 Telephone Messages: Telephone messages and appointment reminders may be left on answering machines and voice mail systems unless the client has requested an alternative means of communication pursuant to DMH Policy No. 500.13, Client Rights to Request Confidential Communication of Protected Health Information (See Reference 2). Each provider and/or clinic should limit the amount of PHI that is disclosed in a telephone message. The content of appointment reminders should not reveal particularly sensitive health information, directly or indirectly. Telephone messages regarding test results or containing information that links a client's name to a particular medical condition should be avoided.

4.1.4 Faxes: The following procedures must be followed when faxing PHI:

- 4.1.4.1 Only the PHI necessary to meet the requester's needs should be faxed.
- 4.1.4.2 Particularly sensitive health information should not be transmitted by fax, except in emergency situations if required by a government agency. If particularly sensitive health information must be faxed, the recipient should be notified immediately prior to the transmission and, if possible, the sender should immediately confirm that the transmission was completed.
- 4.1.4.3 LAC-DMH should designate employees who can fax or approve the faxing of PHI. Unauthorized employees, students, and volunteers should never fax PHI.
- 4.1.4.4 Unless otherwise permitted or required by law, a properly completed and signed authorization must be obtained before releasing PHI to third parties for purposes other than treatment, payment or health care operations as provided in DMH Policy No. 500.01, Use and Disclosure of Protected Health Information Requiring Authorization (See Reference 3). PHI may be faxed to an individual if he/she requests access to his/her own PHI in accordance with DMH Policy No. 500.03, Clients Right to Access Protected Health Information (See Reference 4).
- 4.1.4.5 All faxes containing PHI must be accompanied by a cover sheet that includes a confidentiality notice. Use DMH Fax Cover for Transmitting PHI. (See Attachment 1)



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT:	POLICY NO.	EFFECTIVE DATE	PAGE
SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	500.21	2/15/2013	4 of 7

4.1.4.6 Reasonable efforts should be made to ensure that fax transmissions are sent to the correct destination. Frequently used numbers should be pre-programmed into fax machines or computers to avoid misdialing errors. Pre-programmed numbers should be verified on a routine basis. The numbers of new recipients should be verified prior to transmission.

4.1.4.7 Fax machines must be located in secure areas not readily accessible to visitors and clients. Incoming faxes containing PHI should not be left on or near the machine.

4.1.4.8 Fax confirmation sheets should be reviewed to ensure the intended destination matches the number on the confirmation. The confirmation sheet should be attached to the document that was faxed.

4.1.4.9 All instances of misdirected faxes containing PHI should be investigated and mitigated pursuant to DMH Policy No. 500.17, Mitigation of Harm. (See Reference 5)

4.1.5 Mail: PHI should be mailed within the County's departments in sealed envelopes. PHI mailed outside the County should be sent via first class and should be concealed. Appointment reminders may be mailed to clients unless the client has requested an alternative means of communication pursuant to DMH Policy No. 500.13, Client Rights to Request Confidential Communication of Protected Health Information.

4.2 Physical Safeguards

4.2.1 Paper Records: Paper records containing PHI and clinical records must be stored or filed in such a way as to avoid access by unauthorized persons. Some type of physical barrier should be used to protect paper records from unauthorized access.

4.2.1.1 Paper records and clinical records on desks, counters or nurses stations must be placed face down or concealed to avoid access by unauthorized persons.

4.2.1.2 Paper records should be secured when the office is unattended by persons authorized to have access to paper records.

4.2.1.3 Original paper records and clinical records should not be removed from the premises unless necessary to provide care or treatment to a client or required by law.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	POLICY NO. 500.21	EFFECTIVE DATE 2/15/2013	PAGE 5 of 7
--	---------------------------------	---	---------------------------

- LAC-DMH workforce members should not remove paper records or clinical records for their own convenience.
- Any paper records and clinical records removed from LAC-DMH premises should be checked out according to each program's written internal procedures and should be returned as quickly as possible.
- The safety and return of the medical records checked out or removed are the sole responsibility of the person who checked them out.
- Paper records and clinical records that are removed from LAC-DMH premises must not be left unattended in places where unauthorized persons can gain access.
- Paper records and clinical records must not be left in unlocked automobiles or in view of passers-by.
- The theft or loss of any paper record or clinical record should be reported to the designated Privacy Officer so that mitigation options can be considered.

4.2.2 Destruction Standards: PHI must be discarded in a manner that protects the confidentiality of such information. Paper and other printed materials containing PHI should be destroyed or shredded. PHI or sensitive data stored on media or electronic devices (e.g., diskettes, tapes, zip disks, CDs, DVDs, USB flash drives, and other electronic storage devices) must be deleted or the device destroyed using a DMH approved method.

The LAC-DMH has contracted with a disposal vendor as a business associate to securely pick up, shred or otherwise destroy the PHI. LAC-DMH workforce members must contact DMH Helpdesk and make arrangements to securely transport all media containing PHI to the DMH-Chief Information Office Bureau (CIOB) headquarters. Portable storage media brought in or picked up for disposal will be destroyed by CIOB in accordance to internal media destruction procedures.

4.2.2.1 PHI files and documents awaiting disposal must be stored in containers that are appropriately labeled and are properly disposed of on a regular basis.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	POLICY NO. 500.21	EFFECTIVE DATE 2/15/2013	PAGE 6 of 7
--	---------------------------------	---	---------------------------

- 4.2.2.2 Storage rooms containing confidential information awaiting disposal must be locked after business hours or when authorized staff are not present.
- 4.2.2.3 Centralized bins or containers used for disposed confidential information must be sealed, clearly labeled “confidential,” “PHI” or some other suitable term and placed in a locked storage room.
- 4.2.2.4 Facilities or sites that do not have protected storage rooms or centralized waste/shred bins must implement reasonable procedures to minimize access to PHI.

4.2.3 Physical Access:

- 4.2.3.1 Persons authorized to enter areas where PHI is stored or viewed must wear identifiable LAC-DMH employee badges or be escorted by an authorized County employee.
- 4.2.3.2 Persons attempting to enter an area where PHI is processed must have prior authorizations from LAC-DMH management.
- 4.2.3.3 Employees must not allow others to use or share their badges and must verify access authorization for unknown people entering an area where PHI is stored or processed.

4.2.4 Escorting Visitors or Clients: Visitors and clients must be appropriately monitored when on Department premises where PHI is located to ensure they do not access PHI about other clients without permission. This means that persons who are not part of the LAC-DMH workforce should not be in areas in which clients are being seen or treated or where PHI is stored without appropriate supervision.

4.2.5 Computer/Work Stations: Computer monitors must be positioned away from common areas or a privacy screen must be installed to prevent unauthorized access or observation. Suggested means for ensuring this protection include:

- 4.2.5.1 Use of polarized screens or other computer screen overlay devices that shield information on the screen.
- 4.2.5.2 Placement of computers out of the visual range of persons other than the authorized user.
- 4.2.5.3 Clearing information from the screen when the monitor is not being used.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT:	POLICY NO.	EFFECTIVE DATE	PAGE
SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	500.21	2/15/2013	7 of 7

4.2.5.4 Using password protected screen savers when computer workstations are not in use.

4.3 Technical Safeguards:

4.3.1 Technical safeguards regarding the protection of PHI maintained in electronic form will be developed as part of the efforts to implement security best practices and the HIPAA Security Regulations and will be incorporated into this policy by reference.

4.3.2 Authorized LAC-DMH workforce members may email PHI or Confidential Data when it is first encrypted using the LAC-DMH Secure Messaging Solution. The secure transmission of that email is only available when using approved email systems such as LAC-DMH Outlook, LAC-DMH Outlook Web Access or LAC-DMH Blackberry in accordance with DMH Policy No. 500.49, Appropriate Use of Email for Transmitting PHI and/or Confidential Data. (See Reference 6)

AUTHORITY

1. HIPAA, 45 CFR, Section 164.530 (c)(1)

ATTACHMENT (Hyperlinked)

1. [DMH Fax Cover for Transmitting PHI](#)

REFERENCE

1. DMH Policy No. 307.02, Assignment, Use, and Management of Cellular Devices.
2. DMH Policy No. 500.13, Client Rights to Request Confidential Communication of Protected Health Information.
3. DMH Policy No. 500.01, Use and Disclosure of Protected Health Information Requiring Authorization.
4. DMH Policy No. 500.03, Clients Right to Access Protected Health Information.
5. DMH Policy No. 500.17, Mitigation of Harm.
6. DMH Policy No. 500.49, Appropriate Use of Email for Transmitting PHI and/or Confidential Data.

RESPONSIBLE PARTY

LAC-DMH Compliance Program and Audit Services Bureau, HIPAA Privacy Office